Leaderless Covert Networks

Husslage, B.G.M.; Lindelauf, R.; Hamers, H.J.M.

Publication date:
2012

No. 2012-0057

LEADERLESS COVERT NETWORK: A QUANTITATIVE APPROACH

By

Bart Husslage, Roy Lindelauf,
Herbert Hamers

July 12, 2012

ISSN 0924-7815

Leaderless covert networks: a quantitative approach

Bart Husslage[a] Roy Lindelauf[b] Herbert Hamers[c]

Abstract

Lindelauf et al. (2009a) introduced a quantitative approach to investigate optimal structures of covert networks. This approach used an objective function which is based on the secrecy versus information trade-off these organizations face. Sageman (2008) hypothesized that covert networks organize according to leaderless principles, i.e., clear leaders can not be identified. This flat organizational structure is quite robust to destabilization tactics which target the most important persons in a network. There exist several centrality measures to express the importance of persons in a network. The most recent one introduced in the field of covert networks is a game theoretical centrality measure which takes into account both the structure of the covert network, which usually reflects a communication structure, as well as non-network features, which represent individual parameters like financial means or bomb building skills, see Lindelauf et al. (2011). The question we try to answer in this chapter is whether there is a relationship between the quality of a covert network based on their optimality with respect to the trade-off between secrecy and information and the variance of the game theoretic centrality measures of the respective individuals in the network. The leaderless hypothesis seems to suggest that good covert networks do not have a high distinction between centrality of the individuals, i.e., they are leaderless. We investigate this by looking at homogeneous networks and heterogeneous networks in which the links between individuals are weighted. We find that (approximate) optimal networks have low variance in game-theoretic centrality, i.e., we find evidence that supports the leaderless hypothesis. However, if the networks are heterogeneous in the sense that, for instance, certain individuals communicate much more often than others, we find that the variance increases significantly. Finally, we look at the Jemaah Islamiyah 2002 Bali bombing. We find that the operational network used to conduct and to coordinate the bombing not only facilitated both secrecy and efficiency but also adhered to the leaderless principle.

Keywords: terrorism; network analysis; centrality; game theory.
JEL classification: C71.

[a]Department of Mathematics, Fontys University of Applied Sciences, P.O. Box 90900, 5000 GA Tilburg, The Netherlands.

[b]Military Operational Art & Science, Netherlands Defense Academy, P.O. Box 90002, 4800 PA Breda, The Netherlands.

[c]CentER and Department of Econometrics and Operations Research, Tilburg University, P.O. Box 90153, 5000 LE Tilburg, The Netherlands.

1 Introduction

It is hypothesized that many of the current covert organizations organize according to leaderless principles, see Sageman (2008). According to Dishman (2005) international law enforcement pressure is forcing criminal and terrorist organizations to decentralize their organizational structures, e.g., Mexican law enforcement efforts are causing drug cartels in Mexico to break into smaller units. It is also known that terror organizations exist that are a mix of hierarchical and decentralized structures, i.e., think of Hezbollah and Peru former's Shining Path (cf. Dishman (2005)). Clearly this is done to frustrate intelligence agencies that try to disrupt such organizations by taking out key leaders. If the networks are flat rather than hierarchical it becomes very difficult to determine who the leaders are based on network principles alone. The study of covert networks has received high levels of attention from the modeling community in the last decade. Among others, covert networks have been formally characterized by Tsvetovat and Carley (2005), McAllister (2004) and McCormick and Owen (2000), and their optimal network structures have been analyzed and approximated by Lindelauf et al. (2009a) and Enders and Su (2007). Other approaches concern covert network destabilization strategies, see Farley (2003) and Carley et al. (2003), and tools to identify the most important members of the corresponding organizations, see Koschade (2006), Magouirk and Sageman (2008) and Sparrow (1991).

It is interesting to note that many of the models that focus on covert network structures deal with global network properties, such as their optimality with regard to the secrecy versus information trade-off. The methodology that is being developed to aid in the attack of covert networks, however, focuses on the identification of key players, i.e., is mostly concerned with methods of centrality and thus of a local nature. In this chapter both this global and local approach to covert network modeling will be combined. Recent research points to certain network structures that are more 'optimal' in the sense of balancing the need for secrecy and the ability to exchange information, see Lindelauf et al. (2009a). The question becomes whether such networks still contain 'important' individuals. Clearly, the intuitive answer is that such covert networks do not contain any individual that is much more important than any other individual in the network. The current evolution of global terrorist networks reinforces this statement, i.e., it is well known that many of such networks are flat and do not contain any leaders, see Sageman (2008). The entities making up terrorist networks can be large organizations that work together without any common hierarchy or central commanding authority between them. Whatever the components of the network, what makes it a network is the absence of this central authority or control, see Fukuyama and Shulsky (1997). The question of importance of an individual has been dealt with extensively in the social network domain (cf. Wasserman and Faust (1994)) and has also been applied to the covert network domain, see Lindelauf et al. (2011). In this chapter we investigate the relationship between the variance in game theoretic centrality values of the individuals in the network and the optimality of the respective network. This is interesting because a low variance implies that it becomes hard to identify key players and, henceforth, options for law enforcement to engage the network using kingpin strategies might not be useful. On the other hand, it provides a new measure for the optimality of a covert network.

Essentially we combine two approaches to the analysis of covert networks, i.e., we combine the models that describe the overall covert network topology with the analysis of individual members of those networks. We do this by analyzing centrality in approximate optimal covert network structures. That is, we analyze the centrality values of individuals in both homo-

geneous and heterogenous approximate optimal covert networks. The outline of this chapter is as follows. In Section 2 we introduce the rationale behind covert network models and the various centrality measures that are used to investigate the importance of the individuals in the network. We focus on game theoretic centrality measures, since such measures are able to incorporate additional information about the network and about the individuals involved in the network. We analyze approximate optimal covert networks in Section 3 and the corresponding variance of the game theoretic centrality values of the individuals in the network. In Section 4 we repeat this analysis but now for heterogeneous networks and in Section 5 we apply our method to Jemaah Islamiyah's operational network responsible for the 2002 Bali bombing. We end with a conclusion in Section 6.

2 Covert network models and centrality

In this section we describe the ideas behind a model of covert networks and introduce game theoretic centrality measures. Covert organizations have to make a trade-off between efficient coordination and control on the one hand and maintaining secrecy on the other (cf. Baker and Faulkner (1993)). This is intuitively clear: if everybody in the covert organization knows everybody else, then the security risk to the organization is very high because the exposure of a single individual potentially exposes the entire organization. On the other hand, a very sparsely connected organizational network topology is difficult to coordinate and control, simply because efficient communication between individuals in such an organization is hard. This is quantified by use of an information measure, a secrecy measure, and a balanced trade-off measure, see Lindelauf et al. (2009a). The information measure reflects the fact that the ability to transfer information between individuals in a network is inversely proportional to the number of edges in the shortest path between those individuals. On the other hand, the secrecy measure reflects the fraction of individuals in the network that is expected to remain unexposed upon capture of a single individual according to a realistically chosen probability distribution. Finally, the total performance of a covert organization in dealing with the information versus secrecy trade-off dilemma is reflected by a multi-objective optimization based function. The higher the value of this total performance measure a network attains, the better the network does in balancing secrecy and information. A detailed description of these measures can be found in Appendix A.

Two settings can be considered in constructing the information and secrecy measure. The first setting, the homogeneous case, only considers the communication structure and does not take the nature of interaction into account. The second setting, the heterogeneous case, explicitly takes the nature of interaction into account, since, for example, the frequency or duration of interaction may differ between individuals in a network. This difference is modeled by assigning 'weights' to the links between individuals, representing the risk of that interaction. In Appendix A details of these quantitative measures can be found.

Game theoretic centrality measures can be used to determine the key player in a terrorist network, see Lindelauf et al. (2011). Using such centrality measures we let the value for each possible coalition be defined by the network structure of the coalition. The game theoretic centrality values are obtained by computing the Shapley values (see Shapley (1953)) for the connectivity game v^{conn} (see Appendix A) of the network. This leads to a ranking of the members of the covert organization, with the key players ranked on top. The connectivity game considers coalitions of individuals in the network and their respective lines of communication.

If the members of the coalition are able to communicate using only the links present within the coalition we say that the corresponding subnetwork is connected and assign a value of 1 to the coalition. If not all members in the coalition are able to communicate then we say that the subnetwork is not connected and we therefore assign a value of 0 to this coalition. A coalition consisting of a single individual obtains a value of 0 by definition. The strength of game theoretic centrality measures lies in the fact to incorporate additional information that is available for the coalitions into the modeling. To do so, we introduce a class of weighted connectivity games v^{wconn}. The weight of a coalition now not only depends on the internal communication structure (as presented by the subnetwork formed by the individuals in the coalition) but also on the additional data that is available on the individuals and their relationships present in the respective coalition.

3 Homogeneous networks

In a homogeneous network only the structure of the network is taken into account, i.e., who communicates with whom. Each network of n persons has a balanced trade-off performance measure μ associated with it, see Appendix A. In Lindelauf et al. (2009a) optimal homogeneous networks were derived with respect to this μ-measure for networks up to 7 persons and approximate optimal networks for up to 10 persons. These networks are depicted in Figure 1 and the corresponding μ-values can be found in Table 1.

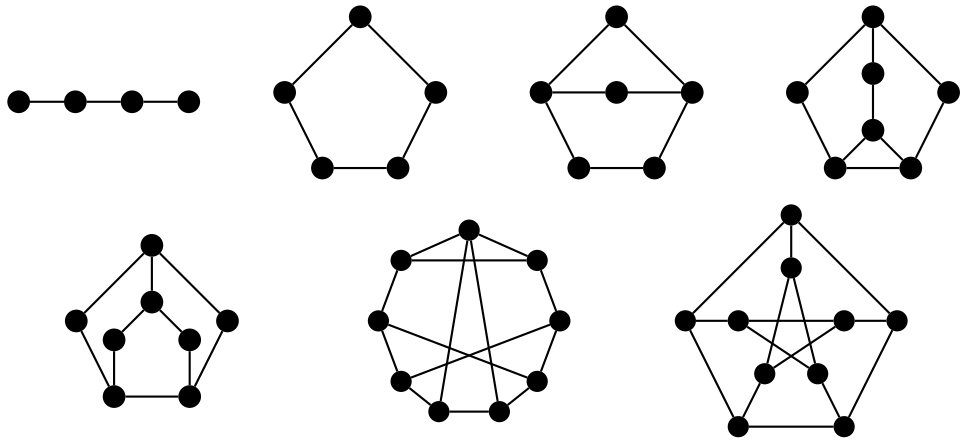

Figure 1: The (approximate) optimal homogeneous networks for $n = 4, \ldots, 10$ persons.

In Lindelauf et al. (2009a) it was shown that covert organizations favor network structures that attain high values of μ. Obtaining game theoretic centrality values for the members of such a network structure, we can construct rankings of the persons involved. The more the centrality values of individuals differ the easier it becomes to differentiate between persons in the ranking. A natural way to quantify differences in individual values by a single number is by computing the variance (denoted by σ^2) of the centrality values. A larger variance then corresponds to a more differentiated ranking. Qualitatively it can be seen that recent covert networks adopt leaderless structures which can be translated to networks that have low variance (i.e., low σ^2) in the centrality values of the respective members of the network. Here we investigate whether covert networks that have high trade-off performance values (μ) attain low values for the variance (σ^2)

in centrality of its members. We expect covert organizations to adopt a network structure with a large value for μ and a small value for σ^2.

A first approach in this chapter is to use simulation techniques to investigate the trade-off between μ and σ^2 for networks up to 10 persons. First we randomly select 10 000 connected networks with n nodes ($n = 4, \ldots, 10$). Then for each network we compute the trade-off performance measure μ and the variance σ^2 of the centrality values. Figure 2 shows the resulting 10 000 pairs (μ, σ^2) for $n = 4, \ldots, 10$. In each chart, the square ($\square$) depicts the pair (μ, σ^2) corresponding to the (approximate) optimal network, as given in Figure 1. The corresponding values of μ and σ^2 for the (approximate) optimal networks are presented in Table 1. Note that $\sigma^2 = 0$ for a regular network, i.e., a network in which each node has the same number of links. This holds, for example, for the regular networks with 5 and 10 nodes, see also Figure 1. A variance of 0, however, does not guarantee an optimal value of μ, see, for example, the optimal networks with 4 and 6 nodes.

n	4	5	6	7	8	9	10
μ	0.2100	0.2667	0.2826	0.3055	0.3229	0.3355	0.3600
σ^2	0.0625	0	0.0069	0.0049	0.0069	0.0009	0

Table 1: Value of μ versus σ^2 for (approximate) optimal homogeneous networks.

Looking at table 1 it can be seen that networks that attain high values for μ indeed have low variance in the centrality of its members. Thus this first simulation approach confirms the conjecture on high μ and low σ^2.

In Figure 3 we show some networks with 9 persons corresponding to different (μ, σ^2) pairs. In network 3(a) all nodes have approximately the same number of links. Hence, the value of σ^2 is small and it is hard to differentiate between persons in the ranking. For a covert network this is a desirable property. However, the large number of links results in a small value of μ, i.e., upon capture of a single individual most of the remaining organization is exposed. Hence it can be concluded that only a low value for σ^2 in the centrality of its members is not necessarily advantageous for a covert organization. If we reduce many of the links we arrive at network 3(b) resulting in a significant improvement of the value of μ. However, now the variance σ^2 in the centrality of the individuals is high, making it easier to identify key members of the organization. A slightly more uniform distribution of the links in network 3(c) takes care of this problem. The number and the placement of links in the approximate optimal network 3(d) not only maximizes the value of μ, but at the same time reduces the variance even further.

4 Heterogeneous networks

In the previous section we analyzed covert organizations by looking at their network structure but ignored the activities that such individuals undertake. In this section we repeat the analysis as presented in the previous section but now we introduce the fact that members of a covert organization interact with one another in different ways. For example, some members may communicate more frequently than other members or may use different (insecure) communication channels. The nature of these interactions may result in a higher risk of exposing (part of) the organization. A heterogeneous network assigns weights to links in the network in order to reflect

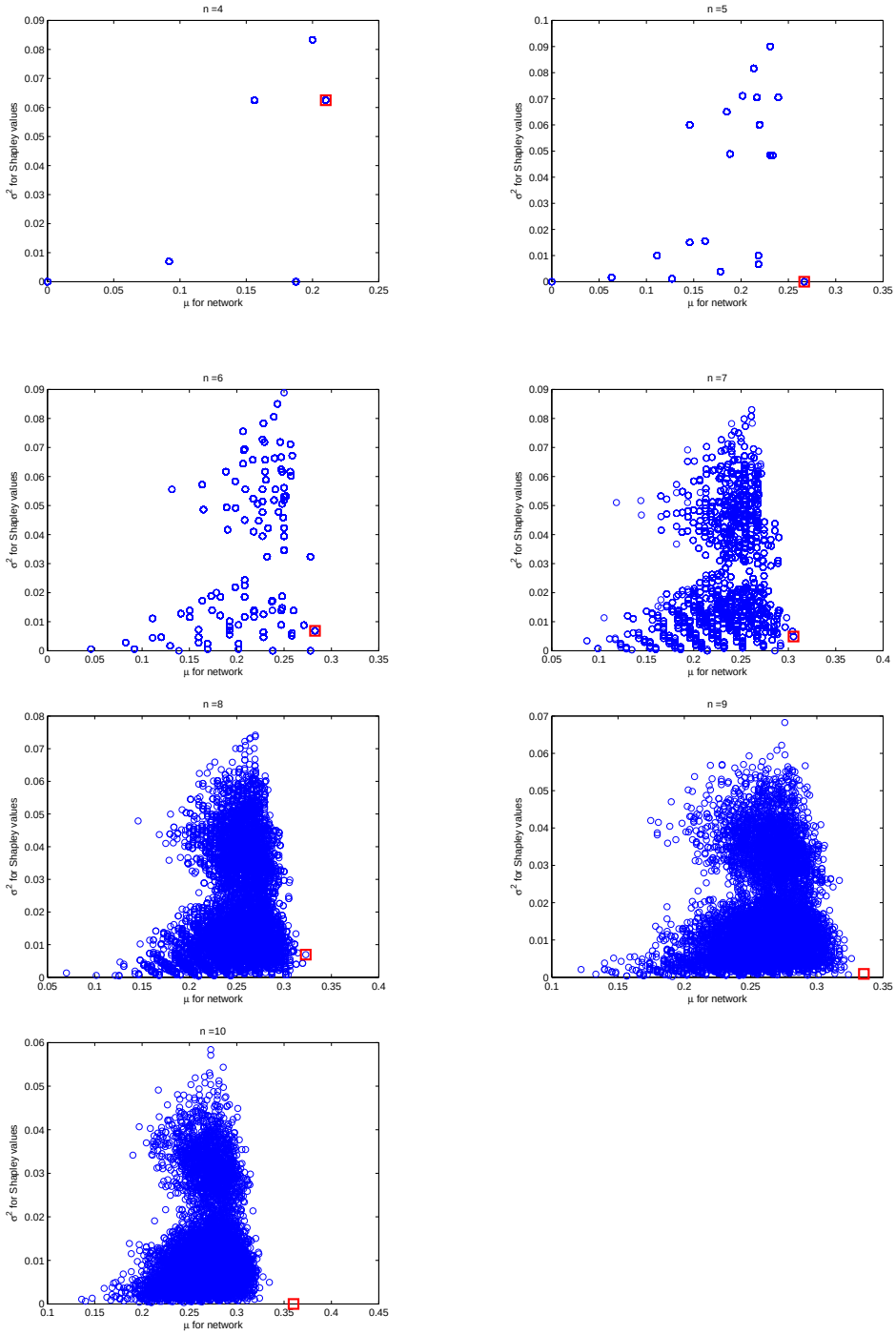

Figure 2: Pairs (μ, σ^2) of 10 000 randomly selected, connected networks of n nodes ($n = 4, \ldots, 10$).

these risks. Lindelauf et al. (2009b) consider networks with a single high risk interaction pair, i.e., heterogeneous networks where exactly one link has a higher weight than the other links.

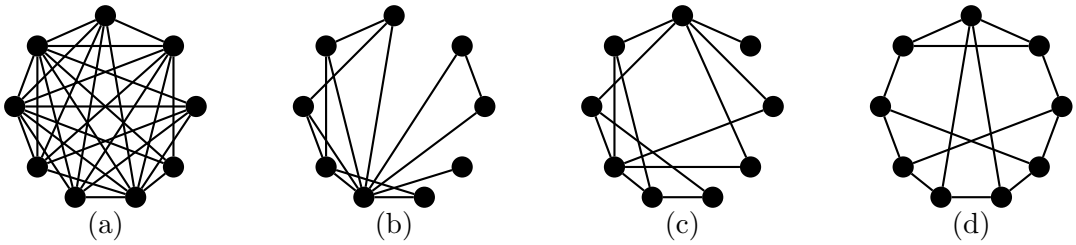

Figure 3: Networks for the (μ, σ^2) pairs $(0.1222, 0.0021)$ (a), $(0.2759, 0.0683)$ (b), $(0.2929, 0.0346)$ (c) and $(0.3355, 0.0009)$ (d).

They show that in this case the high risk interaction pair should have the least connection to the remainder of the network in order to obtain the largest value of the trade-off performance measure μ. Furthermore, they obtain approximate optimal networks for up to 10 nodes using a greedy algorithm and starting from an initial network structure. In these networks the high risk interaction pair is assigned a weight of 2, whereas all other links are assigned a weight of 1. We improve upon these networks by considering the (approximate) optimal homogeneous networks of Figure 1 and selecting the high risk interaction (with a weight of $w = 2$) in each network as stated above. Furthermore, using the simulation techniques of Section 3 no better networks were found, except for the case where the number of nodes is 7 or 8. Figure 4 depicts the resulting networks. In these networks the link with weight 2 is highlighted. In line with the homogeneous case, different (μ, σ^2) pairs will lead to different network structures.

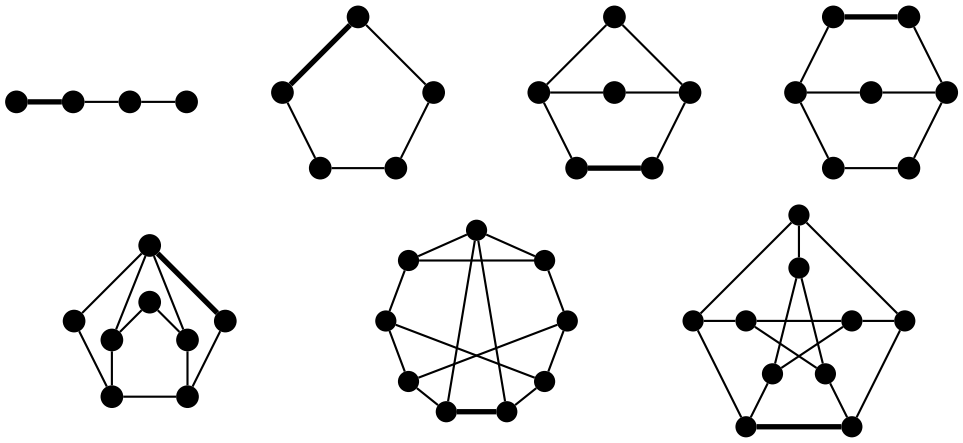

Figure 4: The (approximate) optimal heterogeneous networks (with $w = 2$) for $n = 4, \ldots, 10$ persons.

As in the homogeneous case we investigate the trade-off between the values of μ and σ^2 for networks up to 10 persons. The game theoretic centrality values are obtained by computing the Shapley values for the weighted connectivity game v^{wconn}. This game is a generalization of the connectivity game. If the members of a coalition are able to communicate using only the links present within the coalition we now assign a value equal to the maximal weight of the links present to the coalition. In our case this implies that either a value of 0, 1 or 2 is assigned to each coalition. The variance σ^2 is computed for the centrality values resulting from the Shapley value of the weighted connectivity game. Graphical representations of the pairs

(μ, σ^2), resulting from 10 000 randomly selected, connected networks for $n = 4, \ldots, 10$, closely resemble the ones depicted in Figure 2, and, henceforth, are not repeated here. The values of μ and σ^2 for the (approximate) optimal networks are presented in Table 2.

n	4	5	6	7	8	9	10
μ	0.2125	0.2667	0.2866	0.3067	0.3233	0.3360	0.3600
σ^2	0.1458	0.0483	0.0391	0.0298	0.0418	0.0329	0.0288

Table 2: Value of μ versus σ^2 for (approximate) optimal heterogeneous networks (with $w = 2$).

To investigate the effect of links crucial to the covert network, we consider the above stated heterogeneous case with the difference that the high risk interaction pair is assigned a weight of 10, instead of only 2. Simulation techniques yield the (approximate) optimal networks depicted in Figure 5 and the results in Table 3. Note that the increase of the weight leads to different heterogeneous networks only in the cases of 7 ,8 or 9 nodes. As is to be expected, the variance (σ^2) increases significantly, enabling identification of the important persons in the network. It thus may be concluded that optimal homogeneous network structures are not robust with respect to the addition of high risk interaction pairs. For a covert organization this implies that it should not adopt a static operational structure, but should instead dynamically let its operational structure reflect the current status of its high risk interaction pairs. On the other hand, intelligence agencies should use additional information available on (suspected) members of covert organizations and the relationships present between these members to identify key members of such organizations.

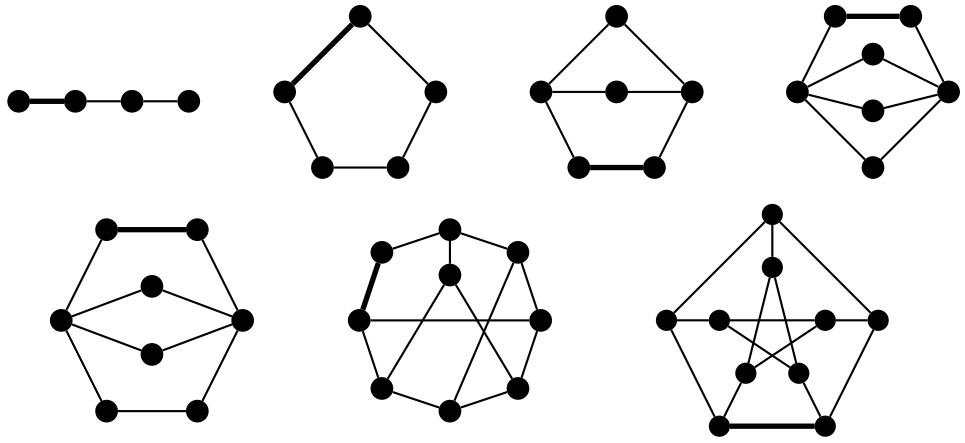

Figure 5: The (approximate) optimal heterogeneous networks (with $w = 10$) for $n = 4, \ldots, 10$ persons.

n	4	5	6	7	8	9	10
μ	0.2196	0.2667	0.3032	0.3214	0.3329	0.3427	0.3600
σ^2	3.8125	3.9150	3.2702	2.9110	2.1520	2.3213	2.3311

Table 3: Value of μ versus σ^2 for (approximate) optimal heterogeneous networks (with $w = 10$).

5 Case: Jemaah Islamiyah's Bali bombing

In the year 2002 the extremist group Jemaah Islamiyah perpetrated one of the deadliest attacks in Indonesia's history. This attack took place on the island of Bali and resulted in the death of 202 people. The operational network conducting the attack consisted of 17 individuals, divided into three teams (cf. Koschade (2006)). Figure 6 depicts the heterogeneous operational network and the three teams: a team of bomb builders (gray), a support team (lightgray) and a team responsible for coordinating the attack (white). Koschade (2006) uses recordings of interaction between members of the network prior to the attack, and in particular the *transactional content* and *frequency and duration* of these interactions, to assign weights between 0 and 5 to each link. In Figure 6 these weights are visualized by the thickness of the lines connecting the individuals in the operational network; i.e., the thicker the line the higher the weight assigned to the corresponding interaction.

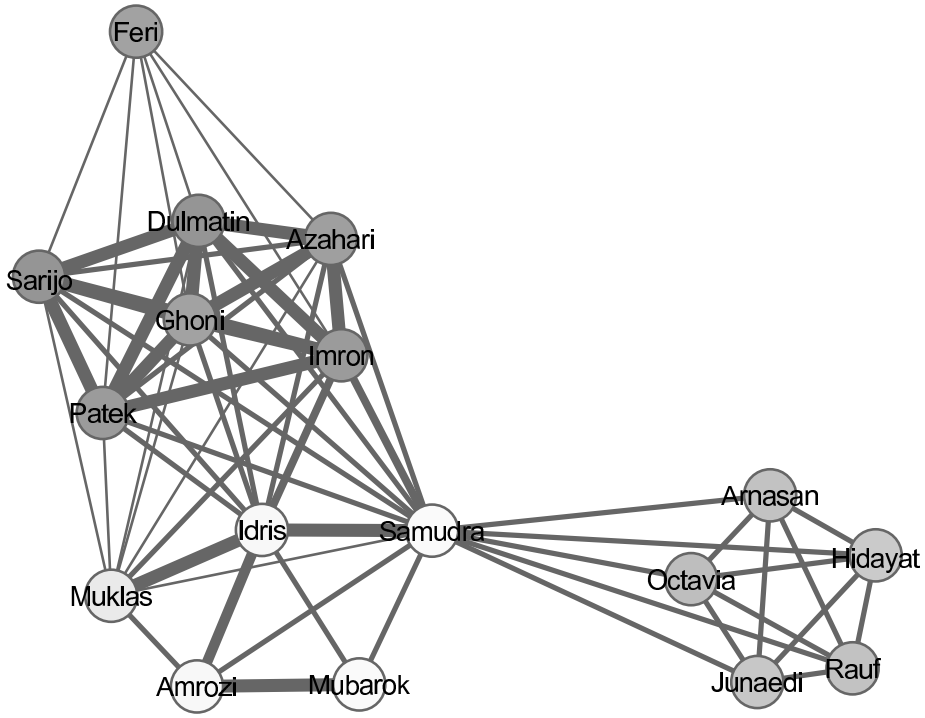

Figure 6: Operational network of Jemaah Islamiyah's Bali attack. Coordination team (white), support team (lightgray) and bomb building team (gray).

Using the weighted connectivity game of Section 4 (but now assigning each coalition a value from 0 up to 5), we find that $\mu = 0.2740$ and $\sigma^2 = 0.8661$. A closer inspection of Figure 6 reveals several high risk interaction pairs, i.e., links with a significant higher weight than the other links. Assume that all lines of communication present in the network were necessary to successfully plan and conduct the attack, i.e., we assume that the network structure is fixed. Using simulation techniques we try to find a distribution of the weights over the links such that the value of μ is maximal. Constructing operational networks with a random distribution of

the weights we find a network with $\mu = 0.2996$ and $\sigma^2 = 2.0120$. Hence, the value of μ increases slightly, whereas the variances increases significantly with respect to the real-world case. On the other hand, searching for a distribution of the weights that minimizes the variance does not result in an improvement (i.e., no network with $\sigma^2 < 0.8661$ is found). From these observations it can be concluded that, given the network structure, the placement of high risk interaction pairs was such that it not only facilitated both the secrecy and efficiency of the operational network but also ensured that the variance among the centrality of the members in the network was small, i.e., it maximized success at avoiding identification of the key members.

6 Conclusion

In this chapter we investigated the conjecture that (approximate) optimal covert networks have low variance in the centrality of their respective members. Qualitative theory hypothesizes that current terrorist networks organize according to leaderless principles. We show that indeed this is optimal, i.e., in Section 3 we show that homogeneous covert networks that are (close to) optimal have low variance in the centrality of their members. However, if we investigate heterogenous networks in which some members have much higher interaction with each other than others then the variance in the centrality increases drastically. Thus for covert networks this implies that they not only should adopt certain network structures, i.e., organize according to leaderless principles, but additionally that they should adopt a communication policy that is flat. Finally, we investigated whether covert organizations actually adopt such a communication policy. We analyzed Jemaah Islamiyah's interaction structure and concluded that the communication policy utilized did indeed closely resemble the optimal flat policy of the given network.

A Methods Summary

A covert network is modelled by a graph $g = (N, E)$, where N represents the set of members of the organization and E represents the links (or relationships) present among these members. We set $|N| = n$ and $|E| = m$. The set of all such networks is indicated by $\mathbb{G}(n, m)$.

Information measure I

The information measure of a graph $g \in \mathbb{G}(n, m)$ is defined by the normalized reciprocal of the total distance in g, i.e.,

$$I(g) = \frac{n(n-1)}{T(g)}.$$

Here $T(g)$ equals the total geodesic distance, i.e., $T(g) = \sum_{(i,j)\in N^2} l_{ij}(g)$ with $l_{ij}(g)$ the geodesic (or shortest) distance between vertex i and vertex j. It follows that $0 \leq I(g) \leq 1$.

Homogeneous secrecy measure $S_{\mathbf{hom}}$

The homogeneous secrecy measure of a graph $g \in \mathbb{G}(n, m)$ is defined by

$$S_{\text{hom}}(g) = \frac{2m(n-2) + n(n-1) - \sum_{i\in N} d_i^2(g)}{(2m+n)n}.$$

Here $d_i(g)$ equals the degree of vertex i in graph g. It follows that $0 \leq S(g) \leq 1$.

Heterogeneous secrecy measure S_{het}

Define the weighting function $w : E \mapsto [1, \infty)$ such that $w_{ij} > w_{kl}$, $ij, kl \in E$, is interpreted as interaction between individuals i and j presenting a higher risk to the organization than interaction between individuals k and l. We denote the set of all such weighting functions by $\mathbb{W}$. Let $w_i = \sum_{j \in \Gamma_i(g)} w_{ij}$ where $\Gamma_i(g) = \{j \in V | ij \in E\}$ and define

$$W = \sum_{i \in V} w_i = 2 \sum_{ij \in E} w_{ij}.$$

The heterogeneous secrecy measure of a graph $g \in \mathbb{G}(n, m)$ is defined by

$$S_{\text{het}}(g) = \frac{n^2 - 2m - n + W(n-1) - \sum_{i \in V} d_i w_i}{n(W + n)}.$$

Balanced trade-off performance measure μ

For $g \in \mathbb{G}(n, m)$ it holds that

$$\mu(g) = I(g)S(g).$$

Game theoretic centrality

A cooperative game is a pair (N, v), where N denotes the set of players. These players can cooperate and form different coalitions. A map v assigns a value $v(S)$ to each possible coalition $S \subseteq N$, which reflects the potential 'power' coalition S represents. By definition $v(\emptyset) = 0$. Let the subgraph S_g consist of the players in coalition S and the lines of communication between these players. If the players in coalition S are able to communicate using only the relationships present within coalition S we say that subgraph S_g is connected and assign a value of 1 to coalition S. If not all players in coalition S are able to communicate then we say that subgraph S_g is not connected and we therefore assign a value of 0 to this coalition. A coalition consisting of a single player obtains a value of 0 by definition. Henceforth, the connectivity game v^{conn} (cf. Amer and Giminez (2004)) is defined as

$$v^{\text{conn}}(S) = \begin{cases} 1 & \text{if } S_g \text{ is connected,} \\ 0 & \text{otherwise.} \end{cases}$$

The game theoretic centrality of player i is found by computing the Shapley value $\varphi_i(v)$ (see Shapley (1953)):

$$\varphi_i(v) = \sum_{S \subseteq N, i \notin S} \frac{|S|!(|N| - 1 - |S|)!}{|N|!} \cdot [v(S \cup \{i\}) - v(S)],$$

where $|S|$ is the number of players in coalition S.

Consider the network depicted in Figure 7. The subgraph corresponding to, for example, coalition $\{A, B, C\}$ is connected, whereas the subgraph corresponding to coalition $\{B, C, D\}$ is not. Hence, $v^{\text{conn}}(\{A, B, C\}) = 1$ and $v^{\text{conn}}(\{B, C, D\}) = 0$. Computing the Shapley values of the 4 players in the connectivity game v^{conn} results in $\varphi_{\text{A}}(v) = 0.6667$, $\varphi_{\text{B}}(v) = 0.1667$, $\varphi_{\text{C}}(v) = 0$ and $\varphi_{\text{D}}(v) = 0.1667$, which leads to the ranking: A, B and D, C.

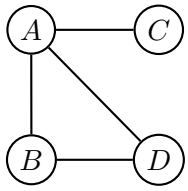

Figure 7: Example of a network of 4 persons.

References

Amer, R. and J.M. Giminez (2004). A connectivity game for graphs. *Mathematical Methods of Operation Research*, **60**, 453–470.

Baker, W.E. and R. Faulkner (1993). The Social Organization of Conspiracy: Illegal Networks in the Heavy Electrical Equipment Industry. *American Sociological Review*, **58**, 837–860.

Carley, K.M., J. Reminga, and N. Kamneva (2003). Destabilizing terrorist networks. *NAACSOS conference proceedings, Pittsburgh*.

Dishman, C. (2005). The leaderless nexus: when crime and terror converge. *Studies in Conflict and Terrorism*, **28**, 237–252.

Enders, W. and X. Su (2007). Rational terrorists and optimal network structure. *Journal of conflict resolution*, **51**, 33–57.

Farley, J.D. (2003). Breaking Al Qaeda cells: a mathematical analysis of counterterrorism operations. *Studies in Conflict and Terrorism*, **26**, 399–411.

Fukuyama, F. and A.N. Shulsky (1997). *The "virtual corporation" and army organization.* RAND corporation.

Koschade, S. (2006). A social network analysis of Jemaah Islamiyah: the applications to counterterrorism and intelligence. *Studies in Conflict and Terrorism*, **29**, 559–575.

Lindelauf, R.H.A., P. Borm, and H.J.M. Hamers (2009a). The influence of secrecy on the communication structure of covert networks. *Social Networks*, **31**, 126–137.

Lindelauf, R.H.A., P. Borm, and H.J.M. Hamers (2009b). *On Heterogeneous Covert Networks.* Springer.

Lindelauf, R.H.A., H.J.M. Hamers, and B.G.M. Husslage (2011). Game theoretic centrality analysis of terrorist networks: The cases of Jemaah Islamiyah and Al Qaeda. *CentER Discussion Paper No. 2011-107*.

Magouirk, J., Atran S. and M. Sageman (2008). Connecting terrorist networks. *Studies in Conflict and Terrorism*, **31**, 1–16.

McAllister, B. (2004). Al Qaeda and the Innovative Firm: Demythologizing the Network. *Studies in Conflict and Terrorism*, **27**, 297–319.

McCormick, G.H. and G. Owen (2000). Security and coordination in a clandestine organization. *Mathematical and computer modeling*, **31**, 175–192.

Sageman, M. (2008). *Leaderless Jihad: Terror Networks in the Twentyfirst Century.* Philadelphia: University of Pennsylvania Press.

Shapley, L. (1953). A value for n-person games. *Annals of Mathematics Studies*, **28**, 307–317.

Sparrow, M. (1991). The application of network analysis to criminal intelligence: An assessment of the prospects. *Social Networks*, **13**, 251–274.

Tsvetovat, M. and K.M. Carley (2005). Structural knowledge and success of anti-terrorist activity: the downside of structural equivalence. *Journal of Social Structure*, **6**.

Wasserman, S. and K. Faust (1994). *Social network analysis, methods and applications.* Cambridge: Cambridge University Press.